~~FILED UNDER SEAL PURSUANT TO THE E-GOVERNMENT ACT OF 2002~~

FILED

OCT 23 2017

CLERK, U.S. DISTRICT COURT
NORFOLK, VA

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated with the email address mizutagod@gmail.com, which is currently stored at premises owned, maintained, controlled, or operated by Dropbox, Inc., a company whose custodian of records is located at 185 Berry St., Suite 400, San Francisco, CA 94107 (Pursuant to 18 U.S.C. § 2703 and Fed. R. Crim. P. 41.)

Case No. 2:17sw176

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: **See Attachment A.**

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*: **See Attachment B.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	*Offense Description*
18 U.S.C. § 2252(a)(2)	Knowingly Receiving or Distributing Child Pornography
18 U.S.C. § 2252(a)(4)	Knowingly Possessing or Accessing With Intent to View Child Pornography

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

David Layne
Special Assistant United States Attorney

Sylvia M. Moreta, Special Agent, NCIS
Printed name and title

Sworn to before me and signed in my presence.

Date: Oct. 23, 2017

City and state: Norfolk, VA

Judge's signature

ROBERT J. KRASK
UNITED STATES MAGISTRATE JUDGE
Printed name and title

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

This warrant applies to information associated with the Dropbox Inc. account mizutagod@gmail.com, to include that information preserved by Dropbox Inc. pursuant to the preservation request made on August 01, 2017, by Special Agent David Masucci pursuant to 18 U.S.C 2703(f), and all electronic digital media that is or was stored in the subject account that is stored at the premises owned, maintained, controlled, or operated by Dropbox Inc., a company whose custodian of records is located at 185 Berry Street, 4th Floor, San Francisco, CA 94107.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Dropbox Inc.:

To the extent that the information described in Attachment B is within the possession, custody, or control of Dropbox Inc., Dropbox Inc. is required to disclose the following information to the government for each account listed in Attachment A:

(a) All information preserved by Dropbox Inc. pursuant to the preservation request made on August 01, 2017, by Special Agent David Masucci pursuant to 18 U.S.C. 2703(f), and all electronic digital media that is or was stored in the subject account.
(b) The contents of all digital media stored in the account, including copies of documents and files shared from or to the account;
(c) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and mean and source of payment (including any credit card or bank account numbers);
(d) All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
(e) All records pertaining to communications between Dropbox Inc. and any person regarding the account, including contacts with support services and records of action taken;

II. Information to be seized by the government

All information described above in Section I and content that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. 2252(a)(2) and 2252(a)(4)(A) and (B) including, for the user ID identified on Attachment A, information pertaining to the following matters:

(a) Content associated with mizutagod@gmail.com that pertains to either the possession, receipt, or sharing of child pornography images or videos.
(b) Any other content pertaining to shared images, pictures, or videos of child pornography.

(c) The attempted or actual production, receipt and possession of child pornography; and

(d) Records relating to who created, used, or communicated with the Dropbox user account associated with mizutagod@gmail.com.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

IN THE MATTER OF THE SEARCH OF THE DROPBOX ACCOUNT LINKED TO MIZUTAGOD@GMAIL.COM

Case No. 2:17sw176

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Sylvia M. Moreta, being duly sworn do depose and state as follows:

1. Since September 2014, I have been a Special Agent with the Naval Criminal Investigative Service (NCIS) and have been assigned to the Norfolk Field Office. NCIS is the investigative arm of the United States Department of the Navy. At NCIS, I am responsible for investigating federal crimes, including crimes against persons, crimes against property, and any other crimes related to the United States Department of the Navy. As part of my regular duties as an NCIS agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have received training in areas investigating crimes utilizing digital media and gathering as well as handling and seizing Digital Evidence. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C 2256(8)) in all forms of media including computer media. I have attended and successfully completed the Federal Law Enforcement Training Center (FLETC) Criminal Investigator Training Program (CITP), the NCIS Special Agent Basic Training Program (SABTP), and the NCIS Advanced Family and Sexual Violence Training Program.

2. As a federal agent, your affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant for information contained in the Dropbox account linked with email address "mizutagod@gmail.com", currently stored at the premises owned, maintained, controlled, or operated, by Dropbox, Inc., a company whose custodian of records is located at 185 Berry St., Suite 400, San Francisco, CA 94107. This affidavit is made in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Dropbox, Inc. to disclose to the Government records and other account information in its possession, pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

4. The statements in this affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents and personnel within the investigative team. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this

RJK
SM

investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. §§ 2252 and 2252A, is located in the Dropbox account associated with "mizutagod@gmail.com."

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. § 2252(a)(4), which makes it a crime to possess child pornography and access child pornography with intent to view it, and violations of 18 U.S.C. § 2252(a)(2), which makes it a crime to receive and distribute child pornography.

LEGAL AUTHORITY

A. Pertinent Criminal Statutes

6. This investigation concerns alleged violations of Title 18 U.S.C. §§ 2252, relating to material involving the sexual exploitation of minors.

7. Title 18 U.S.C. § 2252(a)(2) prohibits a person from knowingly receiving or distributing, using any means or facility of interstate or foreign commerce or that has been mailed, shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed, shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, any visual depiction of minors engaging in sexually explicit.

8. Title 18 U.S.C. § 2252(a)(4) prohibits a person from knowingly possessing, or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed, shipped or transported, by any means including by computer.

B. Other Legal Authority

9. The legal authority for this search warrant application is derived from 18 U.S.C. §§ 2701-2711, entitled "Stored Wire and Electronic Communications and Transactional Records Access." Section 2703(a) provides:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication that is in electronic storage system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication

that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

10. 18 U.S.C. § 2703(b) provides in relevant part:

> (1) A governmental entity may require a provider of a remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent state warrant.
>
> (2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service –
>
> (A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
>
> (B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

11. 18 U.S.C. §§ 2703(b)(1)(A) allows for nationwide service of process of search warrants for the contents of electronic communications and records concerning electronic communication service or remote computing service if such warrant is issued by a court with jurisdiction over the offense under investigation.

12. This investigation involves offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia. *See* 18 U.S.C. § 3237(a); *see also* 18 U.S.C. §§ 3231, 3232. The term "special maritime and territorial jurisdiction of the United States" includes, with respect to offenses committed by a U.S. National, any premises of the United States military missions, including land used for purposes of these missions. 18 U.S.C. § 7(9)(A).

DEFINITIONS

13. The following definitions apply to this affidavit and Attachment B to this affidavit:

14. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital

RJK

image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

14. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

15. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

16. A "minor" is defined as "any person under the age of eighteen years." 18 U.S.C. 2256(1).

17. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

18. "Cloud-based storage service," as used herein, refers to a publicly accessible, online storage provider that collectors of child pornography can use to store and trade child pornography in larger volumes. Users of such a service can share links and associated passwords to their stored files with other traders of child pornography in order to grant access to their collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop and laptop computers, mobile phones, and tablets, anywhere and at any time. An individual with the password to a file stored on a cloud-based service does not need to be a user of the service to access the file. Access is free and readily available to anyone who has an Internet connection.

19. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones and devices. 18 U.S.C. § 1030(e)(1).

20. "File Transfer Protocol" ("FTP"), as used herein, is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

21. "Internet Protocol Address" (IP Address), as used herein, refers to refers to a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every

RJK

SM

time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

22. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called "bandwidth," that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

23. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level or top-level domains are typically ".com" for commercial organizations, ".gov" for the governmental organizations, ".org" for organizations, and, ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government.

24. "Web hosts" provide the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites.Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a Website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting," means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house the customers' hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft or vandalism is greater.

25. "Log Files" are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide

range of events including remote access, file transfers, log-on/log-off times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

26. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

27. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

28. "Uniform Resource Locator" or "Universal Resource Locator" or "URL" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

29. "Electronic Communication Service" refers to any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15).

30. "Remote Computing Service" is a service that provides to the public computer storage or processing services by means of an "electronic communications system." 18 U.S.C. § 2711.

31. "Electronic Communications System" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. 18 U.S.C. § 2510(14).

32. "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8).

33. "Electronic storage" means (a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C. § 2510(17).

RJK

SM

34. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

INFORMATION KNOWN TO AFFIANT REGARDING ELECTRONIC STORAGE

23. As described above and in Attachments A and B, this application seeks authorization to search and seize records that might be found within the Dropbox account associated with mizutagod@gmail.com, in whatever form they are found.

24. With modern internet-capable devices (smartphones, tablets, and computers), metadata, browsing history, and digital media are often stored not only on physical devices, but on the servers of an internet service provider, or "the Cloud."

25. Searching computer systems for the evidence described herein may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the search authorization. Criminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require law enforcement agents, or other analysts with appropriate expertise to conduct more extensive searches, such as scanning areas of the item's memory not allocated to listed files, or peruse every file briefly to determine whether if falls within the scope of the search authorization. In light of these difficulties, NCIS intends to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described herein. Further, I intend to utilize specially-trained computer forensics experts to conduct the search of the subject Dropbox account on an unspecified date, which will be determined by their availability to conduct the search.

INFORMATION KNOWN TO AFFIANT REGARDING CLOUD-BASED COMPUTING AND DROPBOX

26. Cloud computing is a model where computing resources are offered as an internet-based utility. Cloud computing enables access to shared resources, e.g. computer

RJK

SM

networks, servers, storage, applications, etc. over the internet. Dropbox is a cloud-computing resource that acts as a file hosting service.

27. Dropbox, Inc. is a United States-based company headquartered in San Francisco, California that offers cloud storage, file synchronization, personal cloud, and client software. Dropbox utilizes numerous secure, online servers to store subscriber data, files, and folders. Dropbox servers are located in data centers across the United States.

28. Dropbox creates a unique folder on a subscriber's computer, the contents of which may then be synchronized to the Dropbox server, as well as to other computers and devices onto which the subscriber has loaded the Dropbox software. Based on one's subscription plan, Dropbox users may store anywhere from 2 gigabytes to as much as a terabyte of data onto the Cloud. Essentially, Dropbox allows subscribers internet-based file access and storage.

29. Dropbox subscribers can access files and folders (e.g., videos, images, and other digital media) anytime from desktop, web, and mobile clients or applications. These clients are connected to secure servers to provide access to files, file sharing (including peer-to-peer sharing), and to update linked devices when files are added, changed, or deleted. The Dropbox service handles and processes both metadata and raw storage.

30. To subscribe to Dropbox, a user must register with Dropbox. Registration is accomplished by visiting the Dropbox website, inputting a user's full name, email, and a password, and agreeing to the Dropbox Terms of Service. Users then have the option to register for one of several Dropbox service options. Once registered, users may then sync folders and files to the Dropbox server. From then on, the subscriber's account may be accessed by signing in with email address and password.

31. In my training and experience, evidence of who used a Dropbox account, or similar cloud storage service, from when, and where, may be found in the files and records sought herein. This evidence may establish the "who, what, when, where, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish each element of the offense, or alternatively, to exclude the innocent from further investigation.

CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN THE RECEIPT AND POSSESSION OF CHILD PORNOGRAPHY

32. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement colleagues with whom I have had worked and had discussions, I have learned that individuals who view and receive multiple images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children

RJK

may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer, or other digital media storage device or service. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged period. They prefer ready access to their collections. Accordingly, individuals maintaining collections of child pornography frequently maintain said collections on multiple devices or in multiple formats. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

RJK
SM

33. Based on your affiant's training and experience, your affiant knows the following:

a. The development of computers has added to the methods used by child pornography collectors to interact with similarly interested individuals, to download contraband media, and to interact with and exploit children. Computers now allow far easier production, communication, distribution, and storage of child pornography.

b. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communication systems to sell, trade, or market child pornography. Computers have changed this. Modems now allow interconnectivity between computers such that electronic contact can be made easily between millions of computers worldwide. A host computer is one that is attached to a network and serves many users. Such host computers are sometimes operated by commercial providers, such as Microsoft and America Online, which allow subscribers to access network services via connection through an internet broadband provider or by dialing a local number and connecting via a telephone modem.

c. These communications structures are ideal for the child pornography producer and collector. Open and anonymous communication allows users to locate others of similar inclination while maintaining their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other child pornography collectors. Moreover, child pornography collectors can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and distribute pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and anonymous as desired. All of these advantages are well known and are foundations of transactions between modern child pornography collectors.

d. The computer and cloud's capability to store images in digital form makes it an ideal repository for pornography. Where a single floppy disk could store dozens of images and hundreds of pages of text, the size of electronic storage capable in a hard drive or internet-based cloud service has grown tremendously within the last several years. Hard drives and cloud services with the capability to store terabytes-worth of data are common. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with expert examination of electronic storage devices is it possible to recreate the evidence trail.

RJK

e. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

PROBABLE CAUSE TO SEARCH THE SUBJECT ACCOUNT

34. On June 24, 2016, the NCIS Representative to the National Center for Missing and Exploited Children (NCMEC), Special Agent Kea Hartsock, contacted NCIS Special Agent Romy Doria assigned to the NCIS Office in Iwakuni, Japan regarding information provided by Google Inc. on June 17, 2016 and June 22, 2016. Special Agent Hartsock provided NCMEC Cyber Tipline Reports 12515537 and 12644247, which revealed that Google Inc. contacted NCMEC and reported two images of apparent child pornography were uploaded to the Google Gmail account "mizutagod@gmail.com" on June 16, 2016 between 0803 hours and 0804 hours Coordinated Universal Time (UTC). The images were appended to an unsent email in the captioned email account and depicted prepubescent female minors engaged in sexual acts. The upload of the two images to the draft email resolved to IP Address: 153.254.156.155 from a mobile phone with the phone number +15306046103. IP Address: 153.254.156.155 is located on Marine Corps Air Station Iwakuni, Japan, in the special maritime and territorial jurisdiction of the United States. Google Inc. also stated that phone number +15306046103 was the recovery Short Message Service (SMS) added to the account by the user on June 16, 2015. Google Inc. supplied the content of the draft email that contained the uploaded images. The unsent correspondence between "mizutagod@gmail.com" and "yaquar101@wp.pl" read, "I dont have a lot im trieing to get more can i get more vids the ones you sent didnt work a lot pis thanks."

35. In addition to the captioned information, Google, Inc. advised that the Gmail email account "mizutagod@gmail.com" was created in 2014 and "Daniel Mizuta" was the name on the account. Daniel Kamalani Mizuta ("MIZUTA") is an active duty member of the

United States Marine Corps. On all relevant dates in June 2016, MIZUTA worked and resided at Marine Corps Air Station Iwakuni, in Iwakuni, Japan, in the special maritime and territorial jurisdiction of the United States. On June 27, 2016, agents with NCIS interrogated MIZUTA. MIZUTA confirmed that he was the user "mizutagod@gmail.com," and that he had possessed and distributed child pornography using that email account. Also on June 27, 2016, pursuant to a Command Authorization for Search and Seizure, NCIS seized multiple items of electronic media from MIZUTA's on-base residence including a Samsung Galaxy cell phone, a Samsung Tablet computer, and a Dell laptop computer. During a review of the seized media devices, NCIS agents identified four images of suspected child pornography. The images identified are described as follows:

a. IMG.1.1.JPG depicts two prepubescent females lying on a bed. The girls are lying on their backs with underdeveloped breasts exposed, and legs spread to expose the genitals. The girl on the right has the number "1" drawn on her stomach with a lotion like substance. The girl has short blond hair and is smiling facing away from the camera with her hands up in the air. The girl on the right has the number "8" similarly drawn on her body with a white lotion-like substance. The girl has light brown hair with blond streaks and looking at the camera.

b. IMG.8-1.JPG depicts a prepubescent girl with underdeveloped breasts exposed, and legs spread to expose the genitals and portions of her buttocks. The girl is and standing up with her arms placed behind her back. The girl's ribcage and collarbone are protruding. The girl has her eyes closed, with her chin up smiling.

c. IMG.9-1.JPG depicts a single prepubescent girl with underdeveloped breasts exposed, and legs spread apart to expose the genitals. The girl is on top of a blue blanket, which is on top of a bed. The girl is leaning back with her hands facing away from her body to prop her up. The girl is pushing her chest up.

d. IMG.16-1.JPG depicts a prepubescent girl with her eyes closed, underdeveloped breasts exposed, and legs spread apart sitting on a beige couch corner. The girl has her right leg pulled upwards and out close to her chest. The girl is wearing a pink satin pantie with white lace edges. The girl has her right hand placed down the front of her body and into the panties such that her hand is no longer visible. The girl has her left hand bent upwards and tucked under her chin with her head tilted downwards towards the camera. The girl has her eyes closed and mouth slightly parted. It appears the girl is wearing light make up with gold stud earrings. The camera angle is from the side with a white flash.

36. Subsequent to the receipt of information from Google, Inc., the United States Marine Corps returned MIZUTA from Iwakuni, Japan to Virginia Beach, Virginia. MIZUTA currently woks and resides at Naval Air Station Oceana, in Virginia Beach, Virginia, in the Eastern District of Virginia.

37. On July 11, 2017, NCIS requested forensic assistance from the Defense Computer Forensics Laboratory (DCFL) reviewing the above-mentioned digital media devices.

38. DCFL forensic examiner Andrew Siske was assigned the examination. Mr. Siske has worked as a computer forensic examiner for 19 years, 9 of which have been spent at DCFL. He has conducted over 300 examinations and has over 1,500 hours of specialized training in the field of computer forensics. DCFL itself is accredited by the American Society of Crime Lab Directors. Exhibit 1 pertains, and is summarized in the following paragraphs:

a. Upon examination of the Samsung tablet device, Mr. Siske identified approximately 3,000 images of minors in various stages of undress, several of which he described as sexually explicit. One image, file name 240x180_723c515601e2fd5f5860.jpg depicts a mostly-nude adult male and a prepubescent female engaged in a sex act in which the male is lying on his back and the female lying face down on top of the male. The female's right hand can be seen holding the male's erect penis and performing oral sex on the male. File name 160a2ec753298844a61afd4fe4e3e9db.jpg again depicts a mostly-nude adult male, and a nude prepubescent female on a bed. The adult male is kneeling. The minor female is kneeling in front of the male and her face is inches from the male's erect penis.

b. Also identified on the tablet was web history with URLs, which in the experience of Mr. Siske, may pertain to child pornography. The web history includes such URLs as: http://prebabe.biz, http://nakedteens.ru, http://petitepussypics.com, and http://teentinyporn.com.

c. Also identified in the web history of the tablet was the URL: https://www.dropbox.com. The tablet examination was able to identify a Dropbox user account associated with mizutagod@gmail.com and a password "kamalani1."

d. Mr. Siske informed that in his experience, it is not uncommon for individuals to use online file storage for privacy.

CONCLUSION

39. Based on the aforementioned information, your affiant respectfully submits that probable cause exists to believe that the Dropbox account associated with mizutagod@gmail.com, owned by Daniel Kamalani MIZUTA contains child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4), which prohibit the knowing receipt or distribution of visual depictions of and involving the use of a minor engaging in sexually explicit conduct in interstate or foreign commerce, and the knowing possession of or access with the intent to view one or more matters containing any visual depictions of and involving the use of a minor engaging in sexually explicit conduct that have traveled in interstate or foreign commerce or were produced using material so transported or shipped.

40. I further submit that probable cause exists to believe that evidence, fruits, and instrumentalities of such violations will be found within Dropbox account associated with mizutagod@gmail.com, owned by Daniel Kamalani MIZUTA. Accordingly, I request that a warrant be issued authorizing your affiant, with assistance from additional NCIS agents, other law enforcement personnel, and forensic support staff, to search the Dropbox account associated with mizutagod@gmail.com, owned by Daniel Kamalani MIZUTA, for the items specified in Attachment B.

FURTHER AFFIANT SAYETH NOT.

Sylvia M. Moreta, Special Agent
Naval Criminal Investigative Service
Norfolk, VA

Subscribed and sworn before me on ~~September~~ October 23, 2017, in the city of Norfolk, Virginia.

United States Magistrate Judge